BILLY J. WILLIAMS, OSB #901366
United States Attorney
PAUL T. MALONEY, OSB #013366
Assistant United States Attorney
Paul.Maloney@usdoj.gov
GARY Y. SUSSMAN, OSB #87356
Assistant United States Attorney
gary.sussman@usdoj.gov
1000 SW Third Ave., Suite 600
Portland, OR 97204-2902
Telephone: (503) 727-1000
Attorneys for the United States of America

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

PORTLAND DIVISION

UNITED STATES OF AMERICA

v.

STEVEN DOUGLAS ROCKETT,

Defendant.

3:13-CR-00557-SI

GOVERNMENT'S RESPONSE TO DEFENDANT'S MOTION IN LIMINE TO EXCLUDE EVIDENCE RECOVERED FROM UNALLOCATED SPACE, DELETED TRASH, AND RAR FILES

The United States of America, by Billy J. Williams, United States Attorney for the District of Oregon, and Paul T. Maloney and Gary Y. Sussman, Assistant United States Attorneys, responds to and opposes defendant's motion *in limine* seeking to exclude images and other materials recovered from the unallocated space or cache and the "deleted trash" of defendant's digital devices, as well as "RAR" files found on the devices.

Defendant argues that evidence recovered from unallocated space or cache files on a computer is insufficient to support a conviction for knowingly possessing child pornography, absent some evidence that he knew that the cache files existed, or that he had the capability to retrieve them. Because such evidence is insufficient, he argues, it should be excluded at trial. But sufficiency of the evidence to sustain a conviction is a different inquiry from the admissibility of evidence at trial. Defendant's motion should be denied.

I. FACTUAL AND PROCEDURAL BACKGROUND

Defendant is charged in a second superseding indictment with one count of producing child pornography outside of the United States with the intent that it be transported to the United States, in violation of 18 U.S.C. §§ 2251(c) and (e); two counts of engaging in illicit sexual conduct with minors in foreign places, in violation of 18 U.S.C. §§ 2423(c) and (e); five counts of production or attempted production of child pornography, in violation of 18 U.S.C. §§ 2251(a) and (e), and one count of possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). Evidence of those offenses was found in the cache, in unallocated space, and in allocated space on computer equipment and digital data storage media seized from defendant's residence on August 23, 2013, pursuant to a state search warrant. An external hard drive connected to one of defendant's computers was fully encrypted. An internal hard drive in one of the computers has an encrypted container within it. To date, despite extensive decryption efforts, the government has been unable to defeat the encryption and access the data stored on the encrypted drive and the encrypted container.

Defendant is a very sophisticated computer user. He was employed as an information technology professional at Synopsys, a Hillsboro high-technology firm. He worked in the computer technology industry for over a decade. He was running two encryption programs (one of which required *four* passwords to access the encrypted data), an anonymizing

Internet browser to mask his online identity, and a file wiping program to permanently overwrite deleted files in his computer's unallocated space. The file wiping software had been utilized only days before defendant's arrest. He had multiple drives with multiple partitions set up in each drive. He set up encrypted containers within some of the drives. His computer set up was one of the most sophisticated that a forensic examiner who worked on the system had seen.

During the forensic examinations of defendant's digital devices and storage media, evidence was recovered from cache files, from unallocated space, and from the deleted files folder. Such evidence includes:

- Internet browsing history, Internet cache, Internet cookies and emails with account information for "imgsrc.ru" – a Russian-based photo and file sharing site;
- Recovered communications between defendant and an unknown individual(s) relating to defendant inviting another person to view a private Flickr folder called "Then and Now," as well as discussions relating to encryption programs, sharing photos, and TOR – an anonymizing internet browser;
- Recovered registry entries that are system entries of user logins, and software executables (a list of software applications that had been run on the machine);
- Photos recovered from email cache files containing thumbnails of photos of what appear to be naked prepubescent children, some with what appear to have the text "Then and Now" superimposed on the image;

- Recovered video files from an SD card within the Sony Dream Machine hidden camera;
- Recovered and reconstituted video files from an SD card that was in a DVR connected to a pin-hole camera that was hidden in the wall of a bathroom in the defendant's Forest Grove house.

Defendant now seeks to exclude that evidence, along with the contents of a compressed RAR file, from the trial.

II. DISCUSSION

Throughout his motion, defendant refers to files found in a computer's unallocated space or cache as if they are the same thing. They are not. As this Court noted in *United States v. Storm*, 915 F. Supp. 2d 1196 (D. Or. 2012), *aff'd.* 612 Fed. App'x. 445 (9th Cir. 2015), unallocated space is space on a computer's hard drive that contains deleted data, usually emptied from the operating system's trash or recycle bin folder. *Id.* at 1202, n.2 (quoting *United States v. Flyer*, 633 F.3d 911, 918 (9th Cir. 2011)). Files in unallocated space cannot be seen or accessed by a user without the use of forensic software. *Storm,* 915 F. Supp. 2d at 1202, n.2. Even if retrieved, all that can be known about a file found in unallocated space (in addition to the file's contents) is that it once existed on the computer's hard drive; other attributes such as the file creation date, access dates, or the date the file was deleted, cannot be recovered. *Id.* Cache files, on the other hand, are files kept by a web browser to avoid having to download the same material repeatedly, so that images can be redisplayed quickly. *Id.* at 1202, n.3 (quoting *Flyer*, 633 F.3d at 918). A user does not manually save cache files, but can access them and print, rename, or save them elsewhere, much like any other file. *Id.* Finally, files in the deleted trash folder or recycle bin remain in allocated space (and are therefore retrievable by the user) until the trash folder or recycle bin is affirmatively emptied by the user, at which time it is transferred by the computer's operating system to unallocated space. *Id.* at 1202, n.4.

Generally speaking, a defendant cannot be convicted of knowingly possessing child pornography based solely on deleted files found in a computer's unallocated space. *Flyer*, 633 F.3d at 919. On the other hand, a defendant may be convicted of possessing child pornography based on images found in the Internet cache of the defendant's computer, where the defendant admitted seeking out images of child pornography on the Internet, viewing them, saving them to his computer, looking at them for a few minutes, then deleting them. *United States v. Romm*, 455 F.3d 990, 999-1000 (9th Cir. 2006).[1] *See also United States v. Tucker*, 305 F.3d 1193, 1197-98 and 1204-05 (10th Cir. 2002) (affirming the defendant's conviction for possession of child pornography based on images found in the Internet cache, recycle bin, and unallocated space of his computer, where the defendant knew that images from web pages he visited "would be sent to his browser cache file and thus saved on his hard drive," despite his claim that he "did not desire the images to be saved on his hard drive and deleted the images from his cache file after each computer session"). But sufficiency of

[1] To possess images in the cache, a defendant "must, at a minimum, know that the unlawful images are stored on a disk or other tangible material in his possession." *Romm*, 455 F.3d at 1000. In *Romm*, the defendant "exercised control over the cached images while they were contemporaneously saved to his cache and displayed on his screen," viewing them, enlarging some of them, masturbating to them, and eventually deleting them from the cache. *Id.* at 1000-1001.

the evidence to support a conviction and admissibility at trial are two distinct concepts. *Storm*, 915 F. Supp. 2d at 1203.

In *Storm*, the defendant filed a motion *in limine* seeking to exclude images recovered from the unallocated space, the cache, and the deleted trash of his computer equipment and storage media. *Id.* at 1202. Like defendant here, he argued that there was no evidence that he knew the files were present in the unallocated space of his computer or that he had forensic software that would allow him to access those files. *Id.* Like defendant here, Storm argued that he could not be convicted based on those images, at least without additional evidence that he knew of them. *Id.* Accordingly, like defendant here, he sought to exclude their admission at trial.

Like defendant here, Storm relied on sufficiency of the evidence cases to support his motion to exclude the evidence. *Id.* at 1203. This Court, however, held that "the reasoning used to review the accumulation of evidence at the end of a trial cannot be uncritically transposed to evaluating the admissibility of evidence *ex ante*." *Id.* "Whether evidence is ultimately sufficient to sustain a conviction is an entirely different question than whether it is relevant and admissible to establishing a particular element of an alleged offense." *Id.* Where the government sought to introduce files and images from unallocated space or the cache "to help establish Storm's knowing possession of the images," it was "premature to exclude them," even if they would be insufficient standing alone to prove a crime. *Id.* Thus, this Court held that the government "may introduce and use exhibits obtained from unallocated space, Internet search histories ('cache files'), and 'trash' to support its case against Defendant, subject only to the balancing of prejudice and probative value" under Fed. R. Evid. 403. *Id.*

The same result is warranted here. While the evidence defendant seeks to exclude may not be sufficient, standing alone, to convict him of possessing child pornography, there are other counts in the indictment, and other reasons for admitting the evidence. It shows, for example, that defendant has a sexual interest in children. That, in turn, is probative of his motive and his intent to produce and attempt to produce child pornography using cameras hidden in the bathroom of his residence, and his hotel room in the Philippines. It is probative of his motive and his intent in seeking sexually explicit photos from *NS*, as alleged in Count 6, and from *MG* and *HJ*, as alleged in Counts 4 and 5. It gives meaning and context to his requests for "private" photos, "front and back," "from the knees up," and "no shy." It gives meaning and context to the communications between defendant and *NS*, and between defendant and Charis Jumao-as, in which he asks for those photos – communications which could otherwise be interpreted as having an innocuous, non-sexually explicit purpose. And the images found on memory cards taken from a clock radio which contained a hidden camera, and a digital video recorder which controlled a pinhole camera hidden in the bathroom of defendant's residence, are probative of his attempts and intent to produce sexually explicit visual depictions of minors using those cameras, as alleged in Counts 1, 4, 5, 7, and 8.

The nature of the evidence recovered from the unallocated space of the two memory cards further distinguishes this case from other "cache" and "unallocated space" cases. The fact that the two SD cards contained deleted video files is significant to show more than the contents of the media. Those files demonstrate the context and scope of defendant's activities, given the capabilities of each device. The Dream Machine clock radio device did not have the capability to access, display, or edit the contents of the card. The device is motion activated, and will record for a set period of time when there is motion in front of the camera. But in order to delete the files on the card, someone would have to retrieve the card from the device, put it into a computer or other digital data device, and manually delete the files. Therefore, the deleted files prove: 1) that the device created videos; 2) defendant is likely responsible for the images, since he is in some of the recordings, and is seen adjusting the camera angle to capture images of children coming and going from the shower and using the toilet in the bathroom; and 3) defendant, or some other individual, had to remove the SD card from the device in order to access the images and delete them.

The DVR that controlled the bathroom pinhole camera had the ability to access contents of the SD card. That DVR is capable of recording in two modes – "motion activated," and "on." When in "motion activated" mode, the device records for several seconds until the motion stops. When the device is "on," it will record continuously until it is turned "off." Technicians were able to reconstruct the video files from the deleted recordings into continuous recordings, thereby indicating that the DVR was set to "on," rather than "motion activated" mode. Therefore, the deleted files from the DVR SD card are probative to establish: 1) the device created videos; 2) the device was manually set to "on" mode by a user, since the recordings were longer than a few seconds; and 3) the SD card had been accessed by the defendant (or another user), and the content was manually deleted.

The data recovered from the cache and unallocated space of defendant's computer hard drives demonstrates the identity of the user of the computers and how the computer was being used. The Internet cache and browser history show that defendant was seeking out images of naked prepubescent children on imgsrc.ru, selecting images for download, and downloading images to his computer. The government recovered an image of a naked prepubescent boy spread-eagle on a beach from defendant's office computer. The findings from the Internet cache and browser history prove that the defendant's computer accessed this image from imgsrc.ru, and downloaded it directly to his drive the night before his arrest. The government's expert will explain that the browser data was limited on this computer because file wiping software was deleting this data from defendant's computer.

Defendant also seeks to exclude evidence of a RAR file located on his computer. A RAR file is a data container that can store multiple files in a compressed form. *See http://www.rarlab.com/rar_file.htm*, last visited on May 6, 2015. Once downloaded, a RAR file must be "unpacked" using special software called "WinRAR." *Id.* Once unpacked, files can be opened, viewed, printed, and saved to the user's computer or data storage media. *Id.* Defendant claims that "without clear evidence that [he] knew of and accessed the specific images" in the RAR file, "the images should be excluded" (ECF 89 at 6).

That argument suffers from the same analytical flaw as his argument seeking to exclude evidence found in the cache, in unallocated space, and in the trash or recycle bin. It is a sufficiency-of-the-evidence argument, which is not the correct analysis for determining admissibility prior to trial. In any event, WinRAR was installed on defendant's office computer. The computer's desktop had a link to WinRAR, which opened to the directory where the very RAR file defendant seeks to exclude ("*oopreviews.rar*") was found. The computer's registry log demonstrates that defendant regularly used the WinRAR program. He knew of the RAR files on his computer, knew how to unpack them, and regularly used WinRAR to do just that. Assuming the government can establish a proper foundation, the contents of the RAR file found on defendant's computer equipment are admissible at trial, subject to a balancing inquiry under Fed. R. Evid. 403.

III. CONCLUSION

For the reasons set forth above, this Court should follow its prior decision in *Storm* and admit evidence found in unallocated space, cache space, the recycle or trash bin, and in the RAR file at trial, subject to an appropriate balancing inquiry under Fed. R. Evid. 403. Defendant's motion to exclude that evidence should be denied.

Dated this 9th day of May 2016.

Respectfully submitted,

BILLY J. WILLIAMS
United States Attorney

/s/ Paul T. Maloney
PAUL T. MALONEY
Assistant United States Attorney

/s/ Gary Y. Sussman
GARY Y. SUSSMAN
Assistant United States Attorney